WS 08/09 Algebra 1 Musterlösung Blatt 10:

1. Aufgabe:

(a) (i): Sei τ Transposition (ij), σ (n-1)-Zykel, oBdA $\sigma = (2...n)$. Sei zuerst $i = 1$ (oBdA $j = 2$ nach Umordnung):

$$\Longrightarrow \sigma \circ \tau\sigma^{-1} = (31) \text{ bzw. } \sigma^{n-2} \circ \tau\sigma^{-(n-2)} = (n1)$$

Wir wissen aber dass alle Transpositionen der Art $(1i)$ die S_n erzeugen.
(ii): Sei nun $i, j \neq 1$, oBdA $\tau = (2i)$. Da G transitiv operiert, existiert $\psi \in G : \psi(2) = 1$ und daher $\psi(i) = k \neq 1$.

$$\Longrightarrow \tilde{\tau} = \psi \circ \tau \circ \psi^{-1} = (1k)$$

Ersetze nun τ durch $\tilde{\tau}$ und nach dem oberen Fall gilt nun $G = S_n$

(b) Sei $\tau = (ij)$, $\sigma = (1...p)$.
(i) Falls $i, j \in \{1, ..., p\}$ so erzeugen τ, σ als Transposition und p-Zykel die S_p.
(ii) Ist $i \in \{1, ..., p\}, j \notin \{1, ..., p\}$, (oBdA $i = 1$, $j = p + 1$) so gilt nach a) (i) $S_p \subseteq < \tau, \sigma >= S_{p+1}$
(iii) Seien also $i, j \notin \{1, ..., p\}$, oBdA $\tau = ((n-1)(n))$. Da G transitiv gibt es ψ:
$\psi(p) = n, k = \psi^{-1}(n-1) \neq p$. Nun ist $\tilde{\tau} = \psi^{-1} \circ \tau \circ \psi = (pk)$. $\tilde{\tau}$ ist also eine Transposition, von der mindestens ein Element in $\{1, ..., p\}$ liegt und nach einem der oberen Fälle gilt $S_p \subseteq G$.

(iv) In jedem Fall gilt also: $S_m \subseteq G$ mit $m > n/2$.
Da G transitiv operiert, existiert $\psi : \psi(m) = m + 1$. Da $m > n/2$ gibt es $k < m$ mit $\psi(k) = l < m$.
(Denn ψ kann nicht alle Elemente kleiner gleich m auf Elemente größer m abbilden, denn $m > n/2$)
Betrachte nun: $\psi \circ (km) \circ \psi^{-1} = ((m + 1)(l)$ und damit $S_{m+1} \subseteq G$.
Per Induktion folgt nun $G = S_n$.

(c) Sei $f(X)$ aus der Menge $X^4 + 5X^3 + 17X^2 + 15X + 17 + 30\mathbb{Z}[X]$. Sei G die Galois Gruppe über $\mathbb{Q}$
$f(x)$ ist irred mod 2 und damit auch über $\mathbb{Q} \Rightarrow G$ transitiv.
Mod 5 gilt $f(1) = f(4) = 0$ also $f(x) = (X^2 - 1)(X^2 + 3)$ wobei der rechte Faktor irred. (keine NS).
Damit enthält G eine Transposition.
Mod 3 gilt $f(2) = 0$ also $f(x) = (X - 2)(X^3 + X^2 + X + 2)$ wobei wieder der letzte Faktor irred. (keine NS).
Damit enthält G auch einen 3-Zyklus
f mod p ist hierbei jeweils seperabel, da verschiedene Nullstellen abspalten und die irreduziblen Faktoren keine doppelten Nullstellen haben können, da F_p als endlicher Körper vollkommen.

Somit operiert G transitiv, enthält 3 Zyklus und Transposition und ist damit nach a) oder b) gleich der S_n.

(d) Ein solches Polynom muss z.B. genau die Voraussetzungen der Menge in (c) erfüllen, nämlich mod 3 Primzahlen je: irreduzibel sein, einen Linearfaktor abspalten und 2 Linearfaktoren abspalten. Man kann natürlich auch andere Primzahlen nehmen.

2. Aufgabe:

(a) $\mathbb{Q}$ vollkommen, $\Rightarrow K/\mathbb{Q}$ seperabel.

$[\tilde{K} : \mathbb{Q}] = 4$.
$y \notin \tilde{K}$, denn sonst: $[\mathbb{Q}(y) : \mathbb{Q}(\sqrt{2})] = 2$ und daher $y^2 \in \mathbb{Q}(\sqrt{2})$
$\Rightarrow (9 - 5\sqrt{3})(2 - \sqrt{2}) \in \mathbb{Q}(\sqrt{2}) \Rightarrow \sqrt{3} \in \mathbb{Q}(\sqrt{2})$ $\lightning$
$\Rightarrow [K : \mathbb{Q}] = 8$

Wir suchen das Minimalpolynom von y:

Definiere:

$$\begin{aligned} v &= (9-5\sqrt{3})(2-\sqrt{2}) = \alpha^2 \\ w &= (9-5\sqrt{3})(2+\sqrt{2}) = \beta^2 \\ x &= (9+5\sqrt{3})(2-\sqrt{2}) = \gamma^2 \\ y &= (9+5\sqrt{3})(2+\sqrt{2}) = \delta^2 \end{aligned}$$

Es gilt:

$$\begin{aligned} f(X) &= (X^2-v)(X^2-w)(X^2-x)(X^2-y) = X^8 - 72X^6 + 720X^4 - 864X^2 + 144 \\ v \cdot w &= (9-5\sqrt{3})^2(2^2-2) = 312 - 180\sqrt{3} \\ v \cdot x &= (9^2 - 5^2 \cdot 3)(2-\sqrt{2})^2 = 6(6-4\sqrt{2}) \\ v \cdot y = w \cdot x &= 12 \\ w \cdot y &= 36 + 24\sqrt{2} \\ x \cdot y &= 312 + 180\sqrt{3} \\ \alpha \cdot \beta &= 9\sqrt{2} - 5\sqrt{6} \\ \alpha \cdot \gamma &= -\sqrt{6}(-2+\sqrt{2}) \\ \alpha \cdot \delta &= 2\sqrt{3} \\ \beta \cdot \gamma &= 2\sqrt{3} \\ \beta \cdot \delta &= \sqrt{6}(2+\sqrt{2}) \\ \gamma \cdot \delta &= \sqrt{2}(9+5\sqrt{3}) \end{aligned}$$

Man sieht also $f(X) \in \mathbb{Q}(X)$ und $\mathbb{Q}(\sqrt{2}, \sqrt{3}, y) \subseteq \mathbb{Q}(\alpha, \beta, \gamma, \delta)$.
Damit ist K normal als Zerfällungskörper eines Polynoms und somit auch galoisch

(b) Betrachte den Untergruppengraphen von G (aus Blatt 6) Und den Körperturm:

$$\begin{tikzcd} & Id \arrow[d] & \\ & < a^2 > \arrow[dl] \arrow[d] \arrow[dr] & \\ < a > \arrow[dr] & < ab > \arrow[d] & < b > \arrow[dl] \\ & G & \end{tikzcd} \qquad \begin{tikzcd} & L & \\ & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[u] & \\ \mathbb{Q}(\sqrt{2}) \arrow[ur] & \mathbb{Q}(\sqrt{6}) \arrow[u] & \mathbb{Q}(\sqrt{3}) \arrow[ul] \\ & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] & \end{tikzcd}$$

Hierbei ist:

$$a = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Wir wollen die Galois Gruppe nun in die S_n einbetten. Wir wählen also die Zuordnung:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \alpha & \beta & -\alpha & -\beta & \delta & -\delta & \gamma & -\gamma \end{pmatrix}$$

Um $\sqrt{2}$ bzw. $\sqrt{3}$ invariant zu lassen.
Also Motivation: Wir wissen, dass $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ Zwischenkörper, also gibt es Automorphismen

die diese Invariant lassen. Um z.B. $\alpha \cdot -\alpha \cdot \beta \cdot -\beta = \alpha^2 \cdot \beta^2 = v \cdot w = 312 - 180\sqrt{3}$ invariant zu lassen (und damit auch $\sqrt{3}$), permutieren wir $\{\alpha, -\alpha, \beta, -\beta\}$. Für $\sqrt{2}$ analog.

$$g = (1234)(5768)$$
$$h = (1536)(2847)$$

Es soll also gelten: $Fix(< g >) = \mathbb{Q}(\sqrt{3}), Fix(< h >) = \mathbb{Q}(\sqrt{2})$.
Wir müssen nun noch nachrechnen, das g, h wirklich Körperautomorphismen sind. Hier nur für g exemplarisch:
Setze also $g(\alpha) = \beta \Rightarrow g(v) = w \Rightarrow g(vw) = w \cdot g(\beta^2) = 312 \pm 180\sqrt{3}$.
Die Variante mit + kommt wie man oben sieht nicht als Produkt mit w vor $\Rightarrow g(\beta) = \pm\alpha$ und $g(\sqrt{3}) = \sqrt{3}$.
Wäre $g(\beta) = \alpha$ so wäre $\alpha \cdot \beta = 9\sqrt{2} - 5\sqrt{6}$ und damit auch $\sqrt{2}$ invariant, der Fixkörper also $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Diese Invarianz wird allerdings schon durch den Automorphismus $(\alpha \to -\alpha, ..., \delta \to -\delta)$ bewirkt. Da aber
$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ hat die Fixgruppe nur 2 Elemente. $\lightning$
Also $g(\beta) = -\alpha$. Aus $g(\alpha) = \beta, \alpha \cdot \delta = \beta \cdot \gamma = 2\sqrt{3}$ invariant $\Rightarrow g(\delta) = \gamma$
Analog folgt aus $g(\beta) = -\alpha \Rightarrow g(\gamma) = -\delta$

Dies ist nun aber offenbar die gleiche Einbettung wie auf Aufgabenblatt 6 also müssen die Gruppen identisch sein. Insbesondere erzeugen g und h also eine Gruppe der Ordnung 8, wir wissen aber schon, dass die Galois Gruppe Ordnung 8 hat. Wir erhalten also $G \cong Gal(K/\mathbb{Q})$ vermöge $a = g, b = h$.